CS 480/697: Special Topics in Applied Cryptography
Spring 2019 Syllabus

Course Information

- Class room: Wheatley W01-0063
- Class time: MoWeFr 11:00 AM - 11:50 AM
- Class websites: Check Blackboard at `https://umb.umassonline.net/`

Instructor: Dr. Xiaohui Liang

- Email: Xiaohui.Liang@umb.edu
- Office location: Science Building 3rd Floor 80 (S-3-80)
- Office hour: Monday & Wednesday 2:00 PM - 3:00 PM or by appointment
- Office phone number: 617-287-6791

Suggested Textbook and Reading Materials

- (First book) Mihir Bellare and Phillip Rogaway, Introduction to Modern Cryptography, 2005. `http://web.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf`
- (Second book) Shafi Goldwasser and Mihir Bellare, Lecture Notes on Cryptography, 2008. `https://cseweb.ucsd.edu/~mihir/papers/gb.pdf`
- (Third book) W. Stallings. Cryptography and Network Security: Principles and Practices (7th edition). Prentice Hall, 2016, ISBN-13: 978-0134444284 `http://www.inf.ufsc.br/~bosco.sobral/ensino/ine5680/material-cripto-seg/2014-1/Stallings/Stallings_Cryptography_and_Network_Security.pdf`
- W. Mao, Modern Cryptography: Theory and Practice. Prentice Hall PTR, 2003, ISBN: 0130669431
- D. Stinson, Cryptography: Theory and Practice (Third Edition). CRC Press, 2005, 978-1584885085

Course Description

This course aims to introduce the fundamental and practical knowledge of cryptography and its applications. This course covers diverse topics on cryptography and network security techniques including conventional encryption, asymmetric and symmetric cryptology, digital signatures, certificates, key exchange, key management, authentication, network access control, cloud computing security, electronic mail security, advanced crypto primitives, bitcoin, blockchain, and differential privacy. This course focuses on both theoretical aspects and practical applications of cryptanalysis and network security techniques.

Topics Covered

- Security requirements in practical scenarios

- Symmetric encryption
- Finite field and number theory
- Asymmetric encryption
- Diffie-Hellman key exchange
- Hash function, message authentication code, and digital signature
- Key management and distribution
- User authentication
- Network access control and cloud computing security
- Electronic mail security
- New security topics

Course Goals and Learning Objectives

Students successfully completing this course will:

- Understand the fundamental knowledge of the cryptographical technologies
- Understand the security properties of the cryptographical technologies
- Describe the cryptographical technologies
- Identify the vulnerabilities of the cryptographical technologies
- Apply the cryptanalysis skills to evaluate the cryptographical technologies
- Examine the security and privacy challenges of cyber security problems
- Identify the security properties of the cyber security problems
- Apply the cryptographical technologies for cyber security problems
- Explore new cyber security problems with solutions
- Have hands-on experience on implementing security mechanisms

Pre-requisite

CS310

Course Work and Grades

- Project: 25%
- 2 Assignments: 20%
- Midterm exam: 10%
- Final exam for undergraduate students: 45%
- Final exam (30%) and final paper (15%) for graduate students.

Grading Policies

- For project and assignment, no late submissions are accepted unless you have made prior arrangements with me.
- There will be no makeup exam for midterm and final exams.

Grading rubic

$P \geq 90$	A
$90 > P \geq 87$	A-
$87 > P \geq 84$	B+
$84 > P \geq 80$	B
$80 > P \geq 77$	B-
$77 > P \geq 74$	C+
$74 > P \geq 70$	C
$70 > P \geq 67$	C-
$67 > P \geq 64$	D+
$64 > P \geq 60$	D
$60 > P$	F

Accommodations
This class seeks ways to become a working and evolving model of inclusion and universal design for all participants. Individuals with disabilities of any kind (including learning disabilities, ADHD, depression, health conditions), who require instructional, curricular, or test accommodations are responsible for make such needs known to the instructor as early as possible. Every effort will be made to accommodate students in a timely and confidential manner. Individuals who request accommodations must be registered with the Ross Center for Disability Services, which authorizes accommodations for students with disabilities. If applicable, students may obtain adaptation recommendations from the Ross Center for Disability Services, M-1-401, (617-287-7430), `www.rosscenter.umb.edu`. The student must present these recommendations and discuss them with each professor within a reasonable period, preferably by the end of Drop/Add period.

Student Conduct
Students are required to adhere to the University Policy on Academic Standards and Cheating, to the University Statement on Plagiarism and the Documentation of Written Work, and to the Code of Student Conduct as delineated in the catalog of Undergraduate Programs, pp. 44-45, and 48-52. The Code is available online at: `https://www.umb.edu/life_on_campus/policies/community/code`.

Additional information
My emails to the class will be sent from the Blackboard system so make sure that your email address is set up correctly with Blackboard. You should visit the Blackboard website regularly for other information including latest announcements about the class. Make sure you check your UMB e-mail address (usually firstname.lastname001@umb.edu) regularly and/or redirect it to another e-mail address you use more frequently. No excuses regarding infrequent use of this e-mail address will be accepted.

This is a face-to-face course conducted as lectures, presentations and labs. The material will be posted on Blackboard before class time. Students are expected to read class materials before coming to class. Other notes and materials are accessible from Blackboard during class.

Schedule

- Week 1:
  - Course overview: goals and settings, what cryptography is about, and what background do we need?
  - Section 1 of first book and second book.
- Week 2:
  - Symmetric encryption
  - Substitution ciphers, one-time-pad encryption, block ciphers, stream ciphers.
  - Sections 2-5 of first book and Section 4,6 of second book.
- Week 3:
  - Finite field and number theory
  - Section 9-10 of first book.
- Week 4:
  - Asymmetric encryption
  - Section 11 of first book and Section 7 of second book.
- Week 5:
  - Diffie-Hellman key exchange
  - Section 11 of second book
- Week 6:
  - Hash function, message authentication code, and digital signature
  - Sections 6,7,12 of first book and Section 8 of second book.
- Week 7:
  - Midterm review
  - Midterm exam
- Week 8:
  - Crypto protocols: zero knowledge, oblivious transfer, multi-party computation

  - Section 12 of second book

- Week 9:
  - User authentication: password-based, biometric, second factor authentication
  - "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes", IEEE Security & Privacy, 2012.

- Week 10:
  - Network security: IP security and SSL/TLS security
  - Section 16-17 of third book

- Week 11:
  - Electronic mail security
  - Section 15 of third book

- Week 12:
  - Advanced Crypto primitives: Identity-based Crypto, Searchable Encryption, Homomorphic Encryption
  - "Identity-Based Encryption from the Weil Pairing" Crypto 2001.
  - "Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions" Computer and Communications Security 2006.
  - "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes" Eurocrypt 1999.

- Week 13:
  - Bitcoin and block chain
  - "Where Is Current Research on Blockchain Technology?A Systematic Review" 2016
  - "Majority Is Not Enough: Bitcoin Mining Is Vulnerable" Communications of the ACM 2018

- Week 14:
  - Differential privacy
  - "Differential privacy: A survey of results" Cynthia Dwork, 2008.

- Week 15:
  - Course review on crypto theory
  - Course review on crypto applications